Performance Evaluation of L3 Handover Latency in MIPv6

D.Kavitha *, Dr.K.E.Sreenivasa Murthy, S.Zahoor ul Huq

Department of Computer Science & Engineering,
G.Pulla Reddy Engg. College(Autonomous)
Kurnool,Andhra Pradesh,INDIA
dwaramkavithareddy@gmail.com

Abstract

Recent years in the field of mobile communications have brought two significant requirements – seamless service delivery and Quality of Service provisioning. Seamless mobility goes hand in hand with Mobile IPv6 protocol and various handover schemes of this protocol are trying to solve the QoS issue. In this paper we are presenting a method for evaluation of the Layer 3 handover schemes from the handover latency point of view. A L3 handover procedure can be divided into four phases: Movement Detection, CoA Configuration, Home agent Registration and Route Optimization. We simulated the proposed protocol certificate based on Demand Approach in Route Optimization phase and compared it with the return routability procedure in Route Optimization phase of MIPv6 handover. The latencies in different handover phases have been measured in an operated wireless LAN (WLAN) in order to determine the performance bottleneck of handover**.**

1. Introduction

In cellular IP networks, a mobile node (MN) traveling towards a new subnet needs to correctly configure the addresses of its Network Interface Card (NIC) in order to establish and/or
maintain IP layer communications with its peers. To this aim, the MN needs information by Access Router (AR) carried in ICMP messages called RA. Usually the MN initiates handoff process by soliciting an RA message to the new AR. This is the case of *mobile-initiated handoff*. On the other hand, if the ARs (i.e. the network) knew the arrival time of the next handoff instance, the configuration delay of the IP address of the MN could be reduced. This is the case of *network-initiated* handoff[3].

Many researchers proposed different solutions to reduce the time an MN take to complete the handoff process. For example, in [1] the authors suggest to use a learning algorithm to predict future location of MN. The algorithm is based on a Hidden Markov Model and could be used to predict the time arrival of MN to the next Access Point (AP) as well.

In this paper, we propose to use the certificate based On Demand Approach[2] that secures binding updates sent by MN, during Route Optimization. Consequently, we realized that a proper application of this protocol in Route Optimization phase reduces the handoff latency in MIPv6. Moreover, simulations confirm that the handoff setup time tends to be less compared to Return Routability procedure in MIPv6.

The paper is organized as follows. In Section 2, we briefly review handover process in MIPv6 . In Section 3, we illustrate the model used to reduce the handoff delay in MIPv6. Section 4 presents simulation results. Finally, conclusions are drawn in Section 5.

2. Handover in MIPv6

The MIPv6 supports handover that changes its point of attachment to the network when a MN moves to a new IP subnet. The basic handover procedure[4] for the MIP consists of two components, L2 handover and L3 handover. The term L2 handover denotes its support for roaming at the link layer level, while the L3 handover occurs at the network layer level. Usually, the L3 handover is independent of the L2 handover, although it must precede the L3 handover. The MIPv6 handover consists of three operations. These operations may overlap each another. Movement detection which includes L2 handover is a prerequisite procedure for other handover operation. L2 handover that must precede the L3 handover performs channel scanning, authentication, association. A L3 handover procedure can be divided into four phases: Movement Detection, CoA Configuration, Home agent Registration and Route Optimization.

2.1 Movement Detection Phase

Movement Detection phase-handover latency D_{MD} is defined as the time interval between the time when the MN attaches to the new AP (the finish time of L2 handover and that when the MN receives the first RA in the new subnet). D_{MD} *can be calculated as follows*:

$D_{MD} = t1 - t0$ *where* t1 and t0 represents the time point of L2 handover's completion and the time point of the receiving of the first RA respectively.

2.2 Care of address configuration phase

Handover delay D_{DAD} is defined as the time interval between the receiving time of the first RA after the MN attached to the new subnet and the sending time of the first BU from MN to HA. D_{DAD} is calculated as follows

$D_{DAD} = t2 - t1$ *where* t2 represents the first BU sent time.

2.3 Home agent registration phase

Handover delay D_{REG} is defined as the delay time between the MN sends the first BU to the HA and the MN receives the first BA from the HA. D_{REG} is calculated as follows.

$D_{REG} = t3 - t2$ *where t3* represents the first BA received time

2.4 Route Optimization phase

Handover delay D_{RO} *is* defined as the delay between the MN sends the first BU to the CN and the MN receives the first BA from the CN. D_{RO} is calculated as follows

$TO = t4 - t3$ *where t4* represents the first BA received time.

Obviously, the total latency of L3 handover can be calculated as follows.

Handover_delay = $D_{MD} + D_{DAD} + D_{REG} + D_{RO}$

During the handover latency, MN cannot receive any packet from CNs.

3. Certificate Based On-Demand Approach

As in both RR and CBU protocols[6], all the protocol messages in CBOA are carried within IPv6 ''Mobility Header''. The protocol messages exchanged among a MN, its HA and CN are shown in Figure 1. Before a secure BU assured by CN can be sent, the following steps are followed by the three protocol participants. In CBOA, when a MN is roaming to a foreign link, it obtains a CoA as usual and additionally, MN requests a signature on the binding of

(HoA, CoA): $SIG_{HA'} = S_{HA'}$(HoA , CoA , Valid Interval).

In the 1st step, MN first initializes a Binding Update request in Message 1, when it realizes an imminent handover:

Message 1 : Binding Update Request

BUReq : (BU, Nm , HoA , CN).

Message 1 contains MN's own home address, a fresh random nonce, and CN's address in addition to Binding update preparation request (BU). CN's address is included in the message to clearly indicate the destination of the BU request.

HA next does pre-exchanges with CN to prepare the coming binding update through Message 2 and Message 3.

Message 2 : Pre-Information Exchange0

EXCH0 : {Nm , HoA , CN , g^x}.

Message 2 passes the fresh nonce Nm, MN's HoA, CN's address and a DH public value g^x to CN.

Message 3 : Pre-Information Exchange1

EXCH1 : {Nm , Nc , HoA , CN , g^x , g^y , $Cookie_{CN}$}

where CookieCN = prf (K_{CN} , Nm | Nc | HoA | CN | g^x | g^y).

In reply, CN attaches its own fresh nonce N_C and DH public value g^y to the received Message 2 and thus forms Message 3. CN next creates a cookie $Cookie_{CN}$ for HA using its own secret key K_{CN}. CN does not create a state for the protocol to protect itself from resource exhausting attack.

In the next step, MN first proves to HA its ownership of CoA. HA then proves to CN MN's ownership of both its CoA and HoA. A session key is also established between HA (on behalf of MN) and CN to certify the final BU message between MN and CN during the next step. The Diffie Hellman key exchange method is used. This consists of 3 messages.

Message 4. Care-of address Registration:

CoAReg. : {CoA , HoA , Valid Interval , CN , $SIG_{HA'}$, $Cert\ Chain_{HA'}$}.

HA checks the validity of the certificate chain and verifies the signature contained in the message. Negative result of either of them leads to the rejection of the message. Message 4 actually can be a piggy-backed part of MN's care-of address registration message. Note that when the mobile node moves to a different network, and is configured a new care-of address, the mobile node must first register the new care-of address with its home agent together with other operations, before it can use the new care-of address [5].

Inspite of all these security measures, there is a chance for the intruder to also send the similar message on behalf of MN. This attack cannot be determined at this stage as the communication medium between MN and HA itself is not secured. So this type of attacks can be overcome by sending a probe in message 5.

Message 5 : PROBE REQUEST

PROBE_REQUEST : {HoA , CN , Np}

HA sends a PROBE REQUEST to MN's home address to determine if the MN is still in the HoA or not. This message contains MN's own home address, CN's address , a fresh random nonce Np.

In the messages 6 and 7 , a probe request is used to determine the actual location of MN Message 6 : PROBE CONFIRM

PROBE_CONFIRM : {HoA , CN , $PREV\_SIG_1$, $PREV\_SIG_2$, $PREV\_SIG_3$}

This message consists of MN's HoA , CN's address , previous signatures $PREV\_SIG_1$, $PREV\_SIG_2$, $PREV\_SIG_3$.

where $PREV\_SIG_i$ = signature on the last ith data packet received.

If the MN has really moved to the new CoA and if it has sent the BU Request message but not the intruder , HA does not receive any reply packet from MN. But if the MN is still in the HoA and if the BU Request is sent by the intruder , then MN sends a PROBE CONFIRM to the HA.

When the HA does not get a PROBE CONFIRM packet it may be because the MN is not there or the PROBE REQUEST packet may be lost. To handle the latter case it sends a PROBE REQUEST packet after a certain time out. This confirms the availability of MN in its Home address.

Once the HA is clear about the actual location of MN , the next message completes the preparation for the Binding Update. Message 7(a) passes all the required information for Routing optimization to CN, including the information HA obtains in Message 1, the cookie obtained in Message 3 and HA's signature on these information. Finally, HA's certificate chain is also attached.

Message 7(a) : Binding Update Request with Certified (HoA, CoA): {Nm , g^x , $Cookie_{CN}$, HoA , CoA , Valid Interval , CN , SIG_{HA} , $Cert\ Chain_{HA}$}

Where $SIG_{HA} = S_{HA}$ (HoA | CoA | Valid Interval | CN | g^{xy} | Nm | Nc)

On arriving at CN, Message 7(a) is processed in the following sequence: (1) Validate the cookie CookieCN; (2) Check on the authenticity of the certificate chain $Cert\_Chain_{HA}$ (3) Calculate DH key K_{HS}, verify the signature, and check for the equality of the home link subnet prefix strings embedded in both $Cert\_Chain_{HA}$ and HoA.

The included fresh nonce assures the freshness of the signature. If all the results of validation and checking operations are positive, CN now can be confident that both MN's HoA and CoA are indeed correct. At this point, CN creates a cache for (HoA, CoA) and the Binding Update key K_{BU} = prf (g^{xy}, Nm | Nc). Now CN only needs to wait a final message (Message 8) from MN to make sure MN is still alive on its CoA. At the same time, MN obtains the Binding Update key K_{BU} in Message 7(b) from HA and therefore, could send out the final Binding Update message. Note that Message 7(b) is actually sent before Message 7(a) is sent so that Message 8 can be sent earlier.

Message 7(b). Binding Update Reply

BURep : {HoA , CoA , CN , K_{BU}}.

Upon getting K_{BU}, MN now sends out the final message.

Message 8 : Binding Update Message certified by K_{BU}: {HoA , CN , CoA , MAC}

Where MAC = prf (K_{BU} , Nm | HoA | CN | CoA).

Upon receiving Message 8, CN easily verifies that MN is still alive on its CoA. In case that Message 8 arrives at CN before Message 7(a), CN will simply discard it. Considering that buffering Message 8 at CN may cause flooding attacks, we require MN to resend Message 8, if MN still receives data sent by CN from HA. Although this setting may sacrifice the performance a little bit (because of the delay between Message 7(a) and the next Message 8), it helps the proposed protocol to be highly robust against such flooding attacks. Thus, this last step completes the routing optimization protocol.

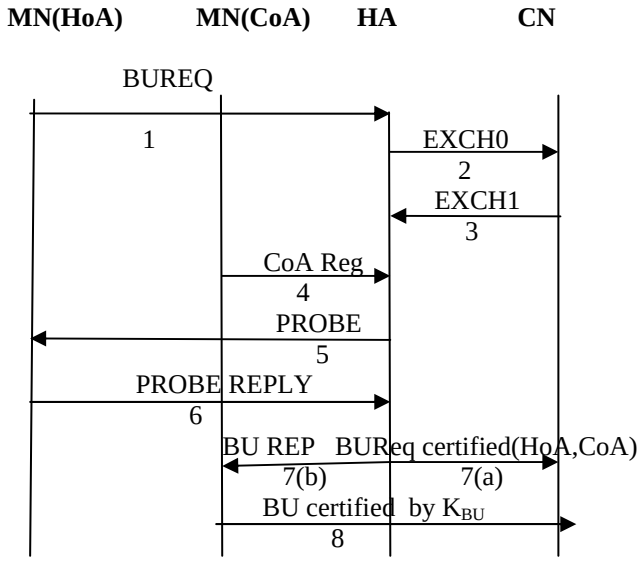

Figure 1 Timing diagram of Certificate Based On-Demand Approach

Note that K_{BU} is the shared secret key to certify the binding update between MN and CN. By making use of K_{BU}, the subsequent Binding Updates between MN and CN can be much more efficient as shown below: Binding Update Message certified by K_{BU} : {HoA , CoA , $SIG_{HA'}$, N'_m , CN , Cert $Chain_{HA'}$, MAC} where MAC = prf (K_{BU} , N'_m | HoA | CN | CoA)

Upon receiving this binding update message, CN first checks the integrity of the attached MAC, and thus verifies the message is indeed sent by MN. Next, CN checks HA's certificate and verifies $SIG_{HA'}$. If both verifications succeed, CN now assures that MN is indeed alive in the CoA as claimed in the previous messages. Further, both MN and CN update K_{BU} = prf (K_{BU} , N' m) in order to prevent replay attack by resending the same message. Note that only one message is needed in this case to accomplish routing optimization between MN and CN.

4. Simulation Results

The handover procedure is repeated 25 times in our experiment using ns2 simulator. The handover latency in every phase is shown below.

4.1 Movement Detection(D_{MD})

MIPv6 defines a new advertisement interval option used in Router Advertisement messages to advertise the time interval Advertisements. D_{MD} is decided by the time interval of router advertisements from the foreign access router. We set the unsolicited multicast Router Advertisement interval to 50ms in order to check the effect of the time interval on D_{MD}. The experimental result is shown as Figure 2. From the figure, we see that the average D_{MD} and maximal D_{MD} are *114.28ms* and *271.14* when the Router Advertisement interval is 50ms. Increasing the sending rate of unsolicited Router Advertisements can reduce D_{MD}, and then MN can detect when it moves to a link served by a new router more quickly. After receiving RA, the MN can acquire a new care-of address and send Binding Updates to register this care-of address with its HA and to notify CNs if necessary.

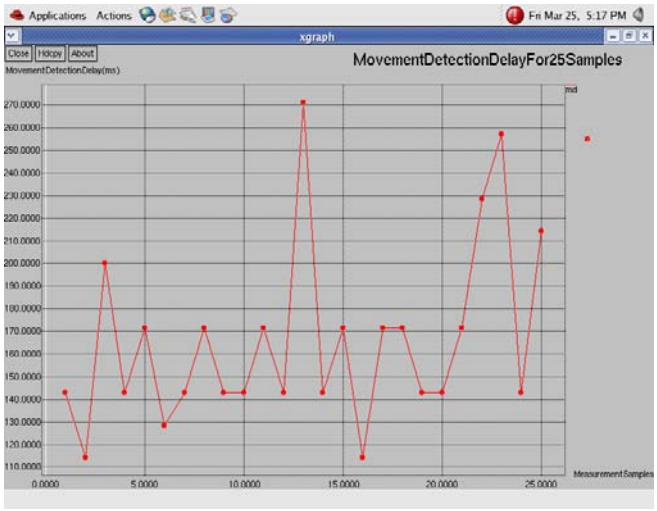

Figure 2 Graph representing Delay in Movement Detection Phase

4.2 Duplicate Address Detection Phase

D_{DAD} is spent in the procedure of forming a new care-of address with either stateless or stateful Address Autoconfiguration when MN moves to a new link. Duplicate Address Detection (DAD) is a necessary procedure for forming an exclusive CoA. RFC 2462 [7] specifies that in normal process of DAD, the MN should delay sending of the initial Neighbor Solicitation message by a random delay time between 0 and MAX_RTR_SOLICITATION_DELAY. Note that after sending Neighbor Solicitation message, the DAD procedure can be considered successful if either no Neighbor Advertisement or other node's Neighbor Solicitation with the same target address is received during a waiting time period which is at least *1000ms* in RFC 2462. Delayed sending and waiting time period can result in significant delays in configuring a new CoA. In our experiment, the time interval from MN sending DAD message to MN sending
Binding Update message to HA is about 1542ms to 2485ms On an average D_{DAD} is 2013 ms The experimental results are shown in figure 3.

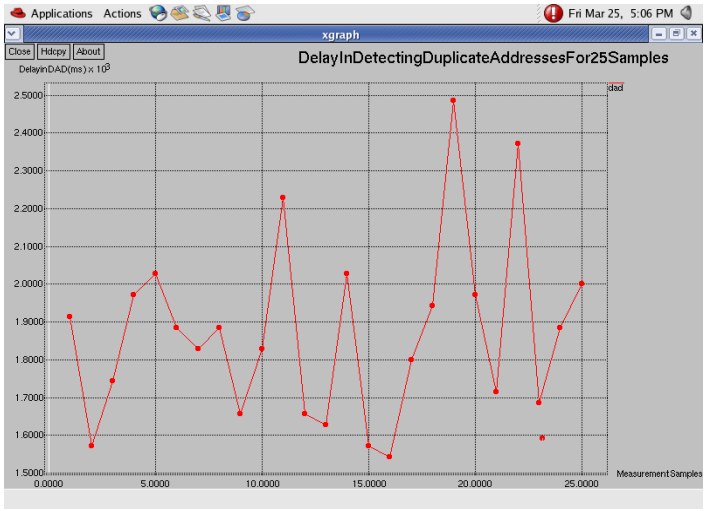

Figure 3 Graph representing Delay in Duplicate Address Detection

4.3 HA Registration Phase

D_{REG} is spent in the home agent registration procedure. It takes more delay time for MN to move from home network to a new subnet than move between two new subnets. The excessive handover time is spent in the DAD procedure of MN's home address by HA in home network. As mentioned earlier, the DAD procedure will result in extra delay time. During the time after the MN sent BU to the HA but before the HA received this BU from MN, a node in home network can use the home address of this MN. The received BU will be rejected by HA for DAD failure if this node uses the home address of this MN. Although the probability of such situation is very small, we can not neglect it.

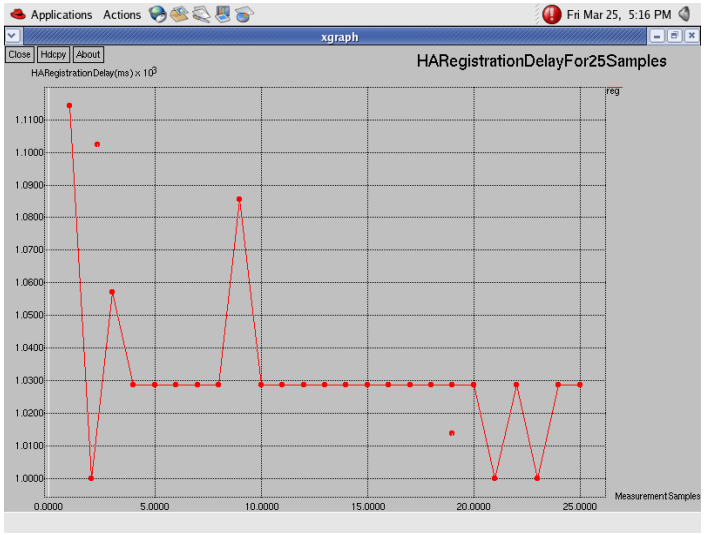

Figure 4 Graph representing Delay in HA Registration Phase

4.4 Route Optimization Phase with Return Routability

D_{RO} includes the time spent on the return routability procedure and the registration time of the MN's new CoA with the CN. The successful registration of HA causes the MN and CN to use bidirectional tunneling to communicate normally. Hence strictly saying, the total L3 handover delay time should not include D_{RO}. On the other perspective, the route optimization procedure eliminates the triangle routing problem, so that it is meaningful to calculate D_{RO} into the total L3 handover delay time. This part of delay time can be reduced by good routing algorithm because of its tight relationship with the network topology . The experimental results are shown n figure 5.

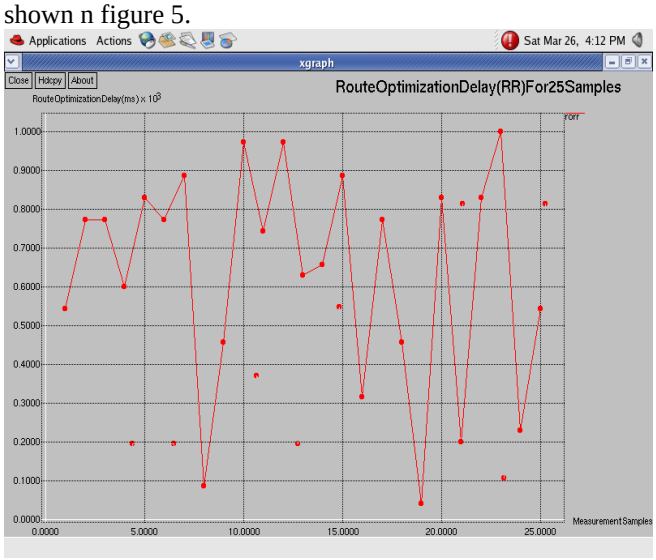

Figure 5 Graph representing Delay in Route Optimization Phase with Return Routabilty procedure

4.5 Route Optimization Phase with CBOA

Certificate Based On-demand Approach is a protocol that secures Binding Updates during RO process. This protocol is further extended to minimize packet losses and reduce hand off latency when a MN moves from one visited network to another.

In the proposed protocol MN initializes BU Request as soon as it realizes an imminent handover. The protocol latency is also significantly reduced as BU Request and pre Information exchange messages are executed right before an imminent handover. If handovers cannot be anticipated, the mobile node may periodically repeat this process, so that they can always be prepared for an unexpected handover.

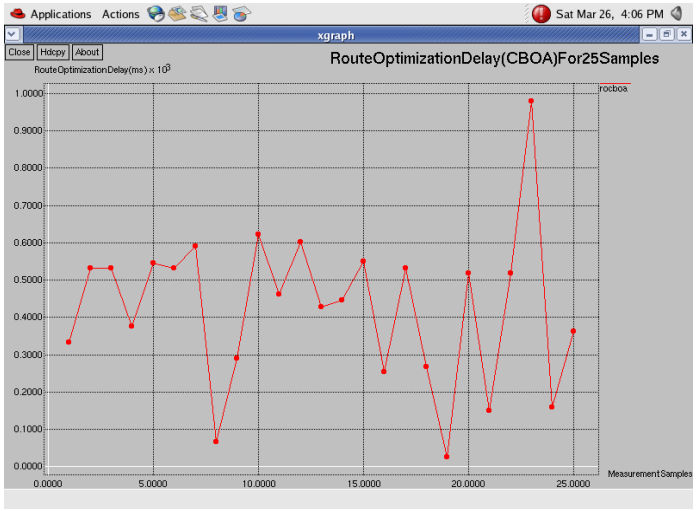

Figure 6 Graph representing Delay in Route Optimization Phase with CBOA

Figure 7 represents the total delay that occurred during the handover process of MIPv6 when RR and CBOA are employed in RO phases respectively.

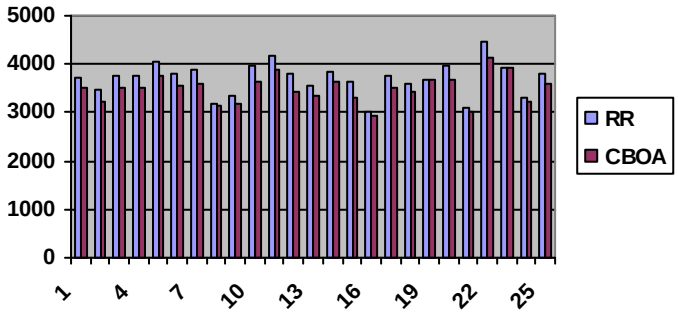

Figure 7. Total handover delay in MIPv6

Conclusion

This paper investigates the latency of different phases in handover procedure of MIPv6 in a WLAN. The phases of Address Autoconfiguration and Home agent registration together produce about 78.8% latency. It is significant to reduce the latency of these two phases to improve the handover performance. Further more, we improve the handover performance and verify the potential of performance enhancement by modifying the protocol implementation of basic MIPv6. If setting the unsolicited multicast Router Advertisement interval to the minimal value, and canceling DAD in Address Autoconfiguration and Home agent registration, the handover latency of basic MIPv6 can be decreased , if do not include the Route Optimization phase, the handover latency can further be decreased. These experimental data also can guide and evaluate the enhancement over MIPv6 to improve the handover performance.

References

[1] J.-M. François and G.Leduc, “Learning movement patterns in mobile networks: a generic approach,” in Proceeding of European Wireless Conference’04, February 2004, pp. 128–134.

[2] D.Kavitha, K.E.Sreenivasa Murthy, B.Sathyanarayana, V.Raghunath Reddy, S.Zahoor-ul-Huq “ Securing Binding Updates in Routing optimizaton of Mobile IPv6”, ICGST-CNIR Journal, Volume 10, Issue 1, December 2010

[3] A.Mishra, M.Shin, and W.A.Arbaugh, “Context caching using neighbor graphs for fast handoffs in wireless network,” in Proceedings of IEEE INFOCOM’04, vol. 23, March 2004, pp. 351–361.

[4] SKOŘEPA, M.; MOLNÁR, K.; KLÜGL, R. Enhanced analytical method for L3 handover cost evaluation. In Proceedings of the 33rd International Conference Telecommunications and Signal Processing. 2010. p. 352 - 357. ISBN 978-963-88981-0-4.

[5] D. Johnson, C. Perkins, and J. Arkko, “Mobility Support in IPv6”, IETF RFC 3775, June 2004, http://www.ietf.org/rfc/rfc3775.txt

[6] K. Ren, W. Lou, K. Zeng, F. Bao, J. Zhou, and R. H. Deng, “Routing optimization security in mobile IPv6,” Computer Networks, vol. 50, no. 13, pp. 2401–2419, 2006.

[7] Thomson, S., Narten, T., "IPv6 Stateless Address Autoconfiguration" RFC 2462, December 1998.

Authors Information

D.Kavitha obatained her B.Tech degree from Sri Krishna Devaraya University, Anantapur and M.Tech degree from Jawaharlal Nehru Technological University, Anantapur in the year 2001 and 2005 respectively. She is currently pursuing Ph.D from Sri Krishna Devaraya University, Anantapur, India. She is presently working as Associate Professor in the Department of Computer Science and Engineering at G. Pulla Reddy Engineering College, Kurnool, Andhra Pradesh, India. She has presented nine research papers in various national and international journals so far Her research areas include Computer Networks and Network Security.

Dr. K.E. Sreenivasa Murthy obtained B.Tech and M.Tech degrees in Electronics and Communication Engineering from Sri Venkateswara University, Tirupati, India in 1989 and 1992 respectively and Ph.D degree from Sri Krishna Devaraya University, Anantapur, India, in 1997. He presented more than 10 research papers in various national and international conferences and journals.He is at present working as principal at Sri Venkateswara Institute Of Engineering and Technology, Anantapur, India. His research interests include FPGA and DSP applications.

S. Zahoor Ul Huq obatained his M.E. degree from Anna University, Chennai he is currently pursuing his Ph.D from Sri Krishna Devaraya University, Anantapur, India. He is presently working as Associate Professor in the Department of Computer Science and Engineering at G. Pulla Reddy Engineering College, Kurnool, Andhra Pradesh, India. He has presented eight research papers in national and international journals so far. His research areas include Computer Networks and Databases and Object Oriented Programming